CLAIMS

1/ A method of making secure the transmission of a message Prgm from an emitter device E to a receiver device R, the method being characterized in that:

- the message Prgm is subdivided into n elementary units I, where n is a number greater than 1;
- a logical property P is defined in such a manner that for any elementary unit I, the logical property P when applied to an authentic elementary unit I gives a logical value of the type true;
- the message Prgm is encrypted by encryption means of the emitter device E using an encryption algorithm having a key Kc so as to obtain an encrypted result Kc(Prgm);
- the encrypted result Kc(Prgm) is transmitted by the emitter device E to the receiver device R;
- the encrypted result Kc(Prgm) is decrypted by the receiver device R using a decryption algorithm having a secret key Kd so as to obtain a decrypted result Kd(Kc(Prgm));
- the decrypted result Kd(Kc(Prgm)) is subdivided into elementary units I;
- the logical property P is applied to the elementary units I so as to obtain, for each unit, a logical value of the type true or of the type false; and
- the message Prgm is considered as being authentic and uncorrupted providing the logical value of each unit is of the type true.

2/ A method according to ~~the preceding claim~~ claim 1, characterized in that the message Prgm is a computer program suitable for being executed and/or interpreted by the receiver device R.

3/ A method according to ~~the preceding claim~~ claim 1, characterized in that the elementary units are instructions of the program Prgm.

4/ A method according to ~~claim 2 or 3~~ claim 1, characterized in that the property P as applied to an elementary unit I gives a logical value of the type true whenever the elementary unit I is executable and/or interpretable.

5/ A method according to ~~claim 2, 3, or 4~~ claim 1, characterized in that the property P as applied to an elementary unit I gives a logical value of the type false whenever the elementary unit I is not executable and/or interpretable.

6/ A method according to ~~any preceding claim,~~ claim 4 characterized in that the receiver device R is a portable object having a memory, of the smart card type.

7/ A method according to ~~any one of claims 1 to 5~~ claim 1, characterized in that the receiver device R includes a portable object having a memory, of the smart card type.

8/ A method according to claim 6, characterized in that the portable object having a memory is a subscriber identity module (SIM).

9/ A method according to ~~any preceding claim,~~ claim 7 characterized in that the message Prgm is written in a high level interpreted language.

10/ A method according to claim ~~9~~ 1, characterized in that the high level language is the Java language.

11/ A method according to claim ~~9 or 10~~ 1, characterized in that the computer program is made up of a set of precompiled instructions.

12/ A method according to ~~any preceding claim,~~ claim 11 characterized in that the message Prgm is encrypted as a continuous flow or in chained-together blocks.

13/ A method according to ~~any preceding claim~~ claim 1, characterized in that the message Prgm is encrypted in blocks, and in that the blocks of the encrypted message Prgm are permutated.

14/ A method according to claim ~~13~~ 1, characterized in that one of the permutated blocks is a starting block or an end block of the message Prgm.

15/ A method according to ~~any one of claims 1 to 12~~ claim 1, characterized in that the result Kc(Prgm) is decrypted in blocks, each encrypted block giving rise to a decrypted block which occupies the same space as the encrypted block.

16/ A method according to ~~any preceding claim~~ claim 1, characterized in that the encryption and decryption algorithms make use of a random number transmitted by the emitter device E to the receiver device R.

17/ A method according to ~~any preceding claim~~ claim 1, characterized in that the message Prgm is recorded, after verification, in a non-volatile memory of the receiver device R.